WEST

Freeform Search

Database: US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Term: L1 and ((compar$ with address$) same (substitute$ with address$))

Display: 10 **Documents in Display Format:** KWIC **Starting with Number** 1

Generate: ○ **Hit List** ◉ **Hit Count** ○ **Side by Side** ○ **Image**

Search | Clear | Help | Logout | Interrupt

Main Menu | Show S Numbers | Edit S Numbers | Preferences | Cases

Search History

12/11 Thursday

DATE: Thursday, December 11, 2003 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; PLUR=YES; OP=ADJ			
L10	L1 and ((compar$ with address$) same (substitute$ with address$))	11	L10
L9	L2 and (compar$ with address$)	7	L9
L8	L2 and (compar with address$)	0	L8
L7	L2 and mac.ab.	0	L7
L6	L2 and L4	0	L6
L5	L2 and (compar$ with address$).ab.	0	L5
L4	L1 and (cable adj1 modem).ab.	38	L4
L3	L2 and (cable adj1 modem).ab.	0	L3
L2	L1 and (protocol adj2 layers).ab.	45	L2
L1	((709/$)!.CCLS.)	17420	L1

END OF SEARCH HISTORY

L9: Entry 4 of 7 File: USPT Jul 28, 1998

DOCUMENT-IDENTIFIER: US 5787253 A
TITLE: Apparatus and method of analyzing internet activity

Abstract Text (1):
An internet activity analyzer includes a network interface controller, a packet capturing module, a packet analysis module, and a data management module. The network interface controller is connected to a transmission medium for a network segment and is arranged to receive the stream of data packets passing along the medium. The packet stream is filtered to remove undesired packet data and is stored in a raw packet data buffer. The packet data is decoded at the internet protocol layer to provide information such as timing and sequencing data regarding the exchange of packets between nodes and the packet data for exchanges between multiple nodes may be recompiled into concatenated raw transaction data which may be coherently stored in a raw transaction data buffer. An application level protocol translator translates the raw transaction data and stores the data in a translated transaction data buffer. The translated data provides high level information regarding the transactions between nodes which is used to monitor or compile statistics regarding network or internetwork activity. The data management module communicates with the packet capturing module and the packet analyzer and, particularly, the data in the raw packet, decoded packet, raw transaction, and translated transaction data buffers to provide real time and stored analytical information concerning internet activity.

Detailed Description Text (26):
Referring now to FIG. 5a, a block diagram of a simplified conventional raw packet data profile 500 is shown to comprise a local network header 505, an internet protocol (IP) header 510, a transmission control protocol (TCP) header 515, application data 520 and a local network trailer 525. The raw packet filter 332 is in communication with other modules such as the IP packet decoder 336 to facilitate the filtering of packets. The packets may be filtered by a variety of data provided in the packet data profile 500, but, preferably, the raw packet filter 332 is set to output data packets for which selected nodes are the source or destination. This facilitates examination of the exchange of data between the selected nodes and any other nodes, whether the other nodes are selected or not. For example two exchanges between first through fourth nodes may be captured. To facilitate such filtering, the raw packet filter 332, in conjunction with, for example, the IP packet decoder 336, decodes a portion of each packet traversing the network medium to which the analyzer 300 is attached. For example the IP source and destination address portions of the data profile 500 may be determined by the raw packet filter 332 to ascertain the raw packet source and destination addresses. This data may then be compared to predetermined address data stored in memory 308. If the predetermined address data matches, for example, the source or destination address data in the packet, the filter 332 stores the packet in the raw packet data buffer 334.

Current US Original Classification (1):
709/231

Current US Cross Reference Classification (4):
709/202

Current US Cross Reference Classification (5):
709/247

CLAIMS:

1. An apparatus for analyzing internet activity, the apparatus comprising:

a packet capturing module, for accessing the packets traversing a network, the packets having source and destination addresses other than an address corresponding to the apparatus, and for filtering the packets to produce raw packet data, wherein the packet capturing module produces the raw packet data by retrieving a predetermined address, comparing the predetermined address to the internet protocol source address for a current packet, comparing the predetermined address to the internet protocol destination address for the current packet, and retaining the current packet where one of the internet protocol source and destination addresses for the current packet matches the predetermined address;

a packet analyzing module, in communication with the packet capturing module, for producing decoded packet data and for producing transaction data from the decoded packet data; and

a data management module, in communication with the packet capturing module and the packet analyzing module, for analyzing at least one of the raw packet data, the decoded packet data and the transaction data to provide an indication of internet usage.

2. An apparatus for analyzing internet activity, the apparatus comprising:

a packet capturing module, for accessing the packets traversing a network, the packets having source and destination addresses other than an address corresponding to the apparatus, and for filtering the packets to produce raw packet data, wherein the packet capturing module produces the raw packet data by retrieving a predetermined port address, comparing the predetermined port address to the transmission control protocol source port address for a current packet, comparing the predetermined port address to the transmission control protocol destination port address for the current packet, and retaining the current packet where one of the transmission control protocol source and destination port addresses for the current packet matches the predetermined port address;

a packet analyzing module, in communication with the packet capturing module, for producing decoded packet data and for producing transaction data from the decoded packet data; and

a data management module, in communication with the packet capturing module and the packet analyzing module, for analyzing at least one of the raw packet data, the decoded packet data and the transaction data to provide an indication of internet usage.

10. For use with an internet activity analyzer capable of being coupled to a network transmission medium, a method of analyzing internet activity, the method comprising:

accessing the packets traversing the network, the packets having source and destination addresses other than an address corresponding to the internet activity analyzer;

filtering the packets to produce raw packet data by retrieving a predetermined address; comparing the predetermined address to the internet protocol source address for a current packet; comparing the predetermined address to the internet protocol destination address for the current packet; and retaining the current packet where one of the internet protocol source and destination addresses for the current packet matches the predetermined address;

producing decoded packet data;

producing transaction data from the decoded packet data; and

analyzing at least one of the raw packet data, the decoded packet data and the transaction data to provide an indication of internet usage.

11. For use with an internet activity analyzer capable of being coupled to a network transmission medium, a method of analyzing internet activity, the method comprising:

accessing the packets traversing the network, the packets having source and destination addresses other than an address corresponding to the internet activity analyzer;

filtering the packets to produce raw packet data by retrieving a predetermined port address; comparing the predetermined port address to the transmission control protocol source port address for a current packet; comparing the predetermined port address to the transmission control protocol destination port address for the current packet; and retaining the current packet where one of the transmission control protocol source and destination port addresses for the current packet matches the predetermined port address;

producing decoded packet data;

producing transaction data from the decoded packet data; and

analyzing at least one of the raw packet data, the decoded packet data and the transaction data to provide an indication of internet usage.

20. An apparatus for analyzing internet activity, the apparatus comprising:

means for accessing the packets traversing the network, the packets having source and destination addresses other than an address corresponding to the internet activity analyzer;

means for filtering the packets to produce raw packet data, wherein the means for filtering the packets to produce raw packet data includes routines for retrieving a predetermined address; comparing the predetermined address to the internet protocol source address for a current packet; comparing the predetermined address to the internet protocol destination address for the current packet; and retaining the current packet where one of the internet protocol source and destination addresses for the current packet matches the predetermined address ;

means for producing decoded packet data;

means for producing transaction data from the decoded packet data; and

means for analyzing at least one of the raw packet data, the decoded packet data and the transaction data to provide an indication of internet usage.

21. An apparatus for analyzing internet activity, the apparatus comprising:

means for accessing the packets traversing the network, the packets having source and destination addresses other than an address corresponding to the internet activity analyzer;

means for filtering the packets to produce raw packet data, wherein the means for filtering the packets to produce raw packet data includes routines for retrieving a predetermined port address; comparing the predetermined port address to the transmission control protocol source port address for a current packet; comparing the predetermined port address to the transmission control protocol destination port address for the current packet; and retaining the current packet where one of the transmission control protocol source and destination port addresses for the current packet matches the predetermined port address;

means for producing decoded packet data;

means for producing transaction data from the decoded packet data; and

means for analyzing at least one of the raw packet data, the decoded packet data and the transaction data to provide an indication of internet usage.

US005787253A

United States Patent [19]

McCreery et al.

[11] Patent Number: 5,787,253

[45] Date of Patent: Jul. 28, 1998

[54] **APPARATUS AND METHOD OF ANALYZING INTERNET ACTIVITY**

[75] Inventors: **Timothy David McCreery**, Lafayette; **Mahboud Zabetian**, Walnut Creek, both of Calif.

[73] Assignee: **The AG Group**, Walnut Creek, Calif.

[21] Appl. No.: **654,347**

[22] Filed: **May 28, 1996**

[51] **Int. Cl.**[6] **H04N 1/413**

[52] **U.S. Cl.** **395/200.61**; 395/200.32; 395/200.77; 370/351; 370/379; 370/389

[58] **Field of Search** 395/200.11, 200.32, 395/200.61, 200.68, 200.75, 200.77; 370/354, 355, 245, 351, 379, 389, 392

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,247,517	9/1993	Ross et al.	370/452
5,315,580	5/1994	Phaal	370/232
5,627,886	5/1997	Bowman	379/111

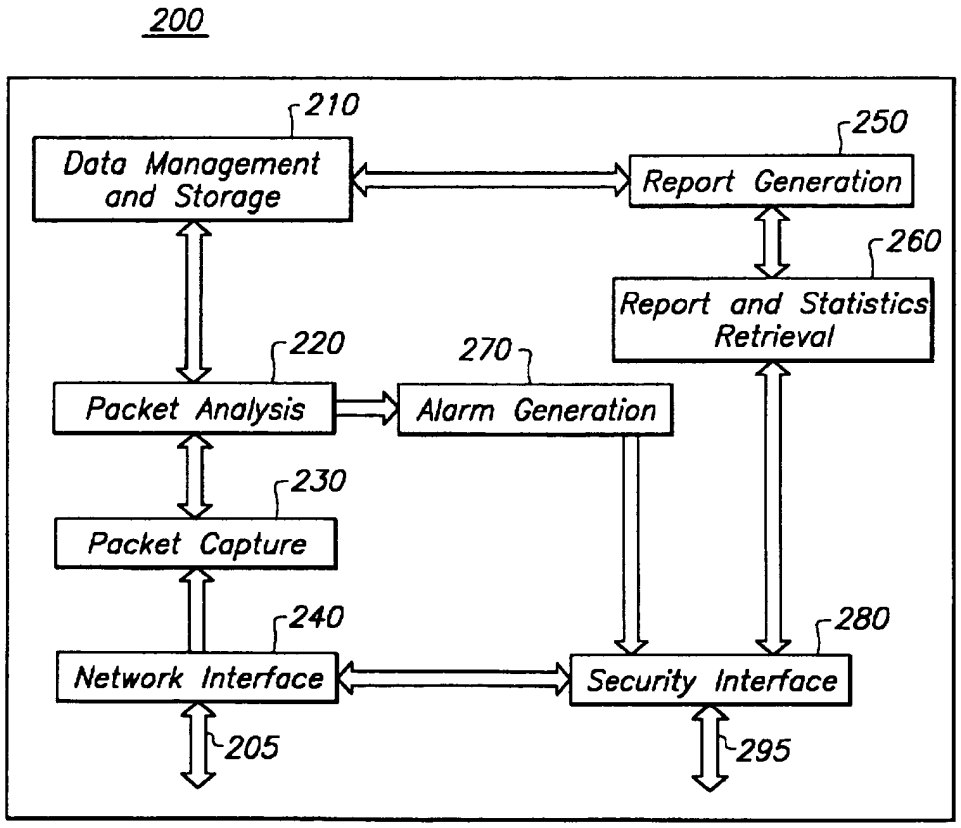
Primary Examiner—Thomas Peeso

Attorney, Agent, or Firm—Fenwick & West LLP

[57] **ABSTRACT**

An internet activity analyzer includes a network interface controller, a packet capturing module, a packet analysis module, and a data management module. The network interface controller is connected to a transmission medium for a network segment and is arranged to receive the stream of data packets passing along the medium. The packet stream is filtered to remove undesired packet data and is stored in a raw packet data buffer. The packet data is decoded at the internet protocol layer to provide information such as timing and sequencing data regarding the exchange of packets between nodes and the packet data for exchanges between multiple nodes may be recompiled into concatenated raw transaction data which may be coherently stored in a raw transaction data buffer. An application level protocol translator translates the raw transaction data and stores the data in a translated transaction data buffer. The translated data provides high level information regarding the transactions between nodes which is used to monitor or compile statistics regarding network or internetwork activity. The data management module communicates with the packet capturing module and the packet analyzer and, particularly, the data in the raw packet, decoded packet, raw transaction, and translated transaction data buffers to provide real time and stored analytical information concerning internet activity.

23 Claims, 12 Drawing Sheets



WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences | Cases

Search Results -

Term	Documents
COMPAR$	0
COMPAR	3614
COMPARA	4023
COMPARAATIVE	3
COMPARAATOR	5
COMPARABALE	5
COMPARABE	7
COMPARABEL	1
COMPARABIE	1
COMPARABIITY	1
COMPARABILITIES	6
(L1 AND ((COMPAR$ WITH ADDRESS$) SAME (SUBSTITUTE$ WITH ADDRESS$))).USPT.	11

There are more results than shown above. Click here to view the entire set.

Database: US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L10

Refine Search

Recall Text | Clear

Search History

DATE: Thursday, December 11, 2003 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; PLUR=YES; OP=ADJ			
L10	L1 and ((compar$ with address$) same (substitute$ with address$))	11	L10
L9	L2 and (compar$ with address$)	7	L9
L8	L2 and (compar with address$)	0	L8
L7	L2 and mac.ab.	0	L7
L6	L2 and L4	0	L6
L5	L2 and (compar$ with address$).ab.	0	L5
L4	L1 and (cable adj1 modem).ab.	38	L4
L3	L2 and (cable adj1 modem).ab.	0	L3
L2	L1 and (protocol adj2 layers).ab.	45	L2
L1	((709/$)!.CCLS.)	17420	L1

END OF SEARCH HISTORY

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 10 of 11 returned.

☐ 1. Document ID: US 6654359 B1

L10: Entry 1 of 11 File: USPT Nov 25, 2003

DOCUMENT-IDENTIFIER: US 6654359 B1
TITLE: Wireless access to packet-based networks

Detailed Description Text (108):
FIG. 24 is a flow diagram illustrating an exemplary procedure for implementing a tunneling optimization at a foreign agent co-located with a corresponding mobile device. In accordance with step 720, when a packet is received at the foreign agent, the IP header checksum is first checked to verify the accuracy of the IP header. In accordance with step 722, a check is made to determine whether the IP Reserved Fragment Flag, included within the IP header, is set. If the IP Reserved Fragment Flag is not set, then the instant packet has not been forwarded to the foreign agent utilizing the tunneling optimization scheme, and normal packet processing is implemented without altering the instant IP packet's destination address. If however, the Reserved Fragment Flag is set, it indicates that the tunneling optimization scheme has been implemented at the home agent and must also be implemented at the co-located foreign agent. Therefore, in accordance with step 724, the instant packet's IP header destination address is compared with entries in the foreign agent's co-located care-of address list. When the mobile device first obtains a care-of address (which is the same as the foreign agent address when the foreign agent is co-located with the corresponding mobile device), the foreign agent updates its care-of address list to reflect the current care-of address. Therefore, if the query made in step 724 returns a negative result, then the instant packet is received in error and the packet is dropped, in accordance with step 730. If however, the instant packet's IP header destination address matches an entry in the foreign agent's co-located care-of address list, then step 726 is performed. In accordance with step 726, the foreign agent substitutes, in the instant packet's IP header destination address, the IP address corresponding to the home agent for the IP address corresponding to the foreign agent (i.e.--the care-of address). In accordance with step 728, packet processing for the instant packet is then resumed at the mobile device.

Current US Cross Reference Classification (4):
709/220

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc | Image

☐ 2. Document ID: US 6643688 B1

L10: Entry 2 of 11 File: USPT Nov 4, 2003

DOCUMENT-IDENTIFIER: US 6643688 B1
TITLE: Method and apparatus for bouncing electronic messages

Detailed Description Text (21):
Preferably, in addition the "from" data is compared to all e-mail addresses in the forwarding database. If the sender address is attached with or from a bounce account, the "from" data is modified to reflect the sender's address "in care of" the bounce system. This can be accomplished in a number of ways, one of which is to create a new temporary e-mail bounce account, referred to as a conversion address. The sender's e-mail address and conversion e-mail address are stored in 107 and 108. The conversion e-mail address is substituted for the sender's address when the e-mail is forwarded. This permits the bounce user to use their "reply" button and have the reply message re-routed through bounce. Upon receipt by bounce, the conversion or "care of" address is changed into a conventional "to" address and the "from" address is adjusted as discussed in 3 below (from a bounce account to a non-bounce account) and the e-mail is sent by the bounce system for delivery.

Current US Original Classification (1):
709/206

Current US Cross Reference Classification (1):
709/219

Current US Cross Reference Classification (2):
709/225

☐ 3. Document ID: US 6442670 B2

L10: Entry 3 of 11 File: USPT Aug 27, 2002

DOCUMENT-IDENTIFIER: US 6442670 B2
TITLE: Data processing system including a shared memory resource circuit

Detailed Description Text (28):
PASS/REMOVAL MODES--In pass mode, a serial stream of 8b/10b encoded characters is received by the optical receiver 34. The data are passed on a serial bus 86 to the deserializer 31 which builds a 20-bit word and recovers the clock. These data are then passed to the Encoder/Decoder (ENDEC) 28 on the HREC_CHAR_INPUT bus 83. The ENDEC 28 assembles the 20-bit subwords into full 40-bit wide words that are then decoded into both command and data. The ENDEC 28 transmits the data on the DEC_DATA bus 76 to the RX_FIFO 25. The commands are sent to the DECODE C-PLD 27, converted into type, and written into TYPE FIFO 24. The Loop Control State Machine (LCSM) 26 detects the data in the RX-FIFO 25. The LCSM routes the data through the FC Data Path FPGA 200 buffers 204 through the DMUX 205 and latches it into HREG 206. This decoded 32 bit word is staged through two registers 203,202 to compare the segment address (bits 39-32) in the segment comparator 201. Simultaneously, the information is clocked into and staged through the Register File 213. The remaining portion of the address (bits 31-12) are sent through the EMUX 212 and staged through a register 211. These address bits are driven out the buffer 215 onto the WADDR bus 70 to the Receive Window Rams 23. The output of the Receive Window Rams 23 are driven over the WIND bus 69 back to the FPGA 200, and are received by an input buffer 217 and driven on an internal bus 260 to a register 218. If the Comparator 201 indicates a `hit`, the packet which has been staged through the register file 213 is directed on RFD 261 to the GMUX 219, with bits 12 through 31 of the address substituted from the window RAM 23 into the address to the GMUX 219. The original address is presented to the FMUX 209 simultaneously.

Current US Cross Reference Classification (1):
709/214

Current US Cross Reference Classification (2):
709/215

☐ 4. Document ID: US 6434134 B1

L10: Entry 4 of 11 File: USPT Aug 13, 2002

DOCUMENT-IDENTIFIER: US 6434134 B1
TITLE: Dynamic address assignment for wireless devices accessing packet-based wired networks

Detailed Description Text (110):
FIG. 24 is a flow diagram illustrating an exemplary procedure for implementing a tunneling optimization at a foreign agent co-located with a corresponding mobile device. In accordance with step 720, when a packet is received at the foreign agent, the IP header checksum is first checked to verify the accuracy of the IP header. In accordance with step 722, a check is made to determine whether the IP Reserved Fragment Flag, included within the IP header, is set. If the IP Reserved Fragment Flag is not set, then the instant packet has not been forwarded to the foreign agent utilizing the tunneling optimization scheme, and normal packet processing is implemented without altering the instant IP packet's destination address. If however, the Reserved Fragment Flag is set, it indicates that the tunneling optimization scheme has been implemented at the home agent and must also be implemented at the co-located foreign agent. Therefore, in accordance with step 724, the instant packet's IP header destination address is compared with entries in the foreign agent's co-located care-of address list. When the mobile device first obtains a care-of address (which is the same as the foreign agent address when the foreign agent is co-located with the corresponding mobile device), the foreign agent updates its care-of address list to reflect the current care-of address. Therefore, if the query made in step 724 returns a negative result, then the instant packet is received in error and the packet is dropped, in accordance with step 730. If however, the instant packet's IP header destination address matches an entry in the foreign agent's co-located care-of address list, then step 726 is performed. In accordance with step 726, the foreign agent substitutes, in the instant packet's IP header destination address, the IP address corresponding to the home agent for the IP address corresponding to the foreign agent (i.e.--the care-of address). In accordance with step 728, packet processing for the instant packet is then resumed at the mobile device.

Current US Cross Reference Classification (2):
709/245

☐ 5. Document ID: US 6389455 B1

L10: Entry 5 of 11 File: USPT May 14, 2002

DOCUMENT-IDENTIFIER: US 6389455 B1
TITLE: Method and apparatus for bouncing electronic messages

Detailed Description Text (21):

Preferably, in addition the "from" data is compared to all e-mail addresses in the forwarding database. If the sender address is attached with or from a bounce account, the "from" data is modified to reflect the sender's address "in car eof" the bounce system. This can be accomplished in a number of ways, one of which is to create a new temporary e-mail bounce account, referred to as a conversion address. The sender's e-mail address and conversion e-mail address are stored in 107 and 108. The conversion e-mail address is substituted for the sender's address when the e-mail is forwarded. This permits the bounce user to use their "reply" button and have the reply message rerouted through bounce. Upon receipt by bounce, thw conversion or "care of" address is changed into a conventional "to" address and the "from" address is adjusted as discussed in 3 below (from a bounce account to a non-bounce account) and the e-mail is sent by the bounce system for delivery.

Current US Original Classification (1):
709/206

Current US Cross Reference Classification (1):
709/225

Current US Cross Reference Classification (2):
709/329

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 6. Document ID: US 6308200 B1

L10: Entry 6 of 11 File: USPT Oct 23, 2001

DOCUMENT-IDENTIFIER: US 6308200 B1
TITLE: Method for connecting terminals to a host computer and a host computer therefor

Detailed Description Text (12):
Furthermore, other embodiments can be considered, in which a reference version number, for example, V. 2.0, may be input as a substitute of the renewal date in step S91 in FIG. 10, then the host computer reads the forum name BASEBALL and the version number V. 2.0 in step S93 in FIG. 10 and determines whether or not the updated version number, for example, V. 3.0, addressed to the forum BASEBALL, which is newer than the version number V. 2.0, has been received and rewritten on the electronic bulletin board. Then, the updated version number V. 3.0 read from the information addressed to the forum name BASEBALL is compared with the reference version number V. 2.0. The log-in process is executed if the updated version number, for example, V. 3.0 is newer than the version number V. 2.0, and the log-out process is executed if the read version number, for example, V. 2.0 is not newer than the version number V. 2.0.

Current US Original Classification (1):
709/206

Current US Cross Reference Classification (1):
709/227

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc | Image

---

☐ 7. Document ID: US 6256722 B1

L10: Entry 7 of 11 File: USPT Jul 3, 2001

DOCUMENT-IDENTIFIER: US 6256722 B1
TITLE: Data processing system including a shared memory resource circuit

Detailed Description Text (27):
PASS/REMOVAL MODES--In pass mode, a serial stream of 8b/10b encoded characters is received by the optical receiver 34. The data are passed on a serial bus 86 to the deserializer 31 which builds a 20 bit word and recovers the clock. These data are then passed to the Encoder/Decoder (ENDEC) 28 on the HREC.sub.13 CHAR.sub.13 INPUT bus 83. The ENDEC 28 assembles the 20-bit subwords into full 40-bit wide words that are then decoded into both command and data, The ENDEC 28 transmits the data on the DEC.sub.13 DATA bus 76 to the RX.sub.13 FIFO 25. The commands are sent to the DECODE C-PLD 27, converted into type, and written into TYPE FIFO 24. The Loop Control State Machine (LCSM) 26 detects the data in the RX-FIFO 25. The LCSM routes the data through the FC Data Path FPGA 200 buffers 204 through the DMUX 205 and latches it into HREG 206. This decoded 32 bit word is staged through two registers 203,202 to compare the segment address (bits 39-32) in the segment comparator 201. Simultaneously, the information is clocked into and staged through the Register File 213. The remaining portion of the address (bits 31-12) are sent through the EMUX 212 and staged through a register 211. These address bits are driven out the buffer 215 onto the WADDR bus 70 to the Receive Window Rams 23. The output of the Receive Window Rams 23 are driven over the WIND bus 69 back to the FPGA 200, and are received by an input buffer 217 and driven on an internal bus 260 to a register 218. If the Comparator 201 indicates a `hit`, the packet which has been staged through the register file 213 is directed on RFD 261 to the GMUX 219, with bits 12 through 31 of the address substituted from the window RAM 23 into the address to the GMUX 219. The original address is presented to the FMUX 209 simultaneously.

Current US Cross Reference Classification (1):
709/213

Current US Cross Reference Classification (2):
709/214

Current US Cross Reference Classification (3):
709/215

☐ 8. Document ID: US 6000020 A

L10: Entry 8 of 11 File: USPT Dec 7, 1999

DOCUMENT-IDENTIFIER: US 6000020 A
TITLE: Hierarchical storage management from a mirrored file system on a storage network segmented by a bridge

Detailed Description Text (98):
Returning to the consideration of step 718 in FIG. 8B, suppose the left half Bridge local OPN was found to be of higher priority. In this case, it is necessary to close the remote source, look up the location of the destination node of the winning local OPN, possibly convert the winning OPN back to half duplex if it is pseudo-full-duplex and its destination is local, and forward the winning OPN on the appropriate path. This process is started in step 740 on FIG. 8C. This step represents the process of accessing the memory 78 in FIG. 5 to determine if the destination node of the winning OPN is local or remote. This is done by the RX Port

State. Machine by activating the Read signal on line 110 in FIG. 7. When the local OPN arrived at pint of the RX port, Decode circuit 620 recognized it as an OPN and activated the OPN signal on line 654 and activated the Latch [0:1] signal on line 656. The Latch [0:1] signal caused the AL.sub.-- PA latch 200 to latch the source and destination addresses. If the incoming OPN was a half-duplex, Decode circuit 620 also activated the Half Duplex signal on line 658. The activation of OPN and Half Duplex causes RX Port State Machine to activate the RX Convert signal on line 660. This causes the AL.sub.-- PA latch circuit 200 to substitute hex F7 or F8 for the source address in the AL.sub.-- PA address stored therein. The address stored in latch 200 is presented on bus 108 to both memory 78 and comparator 402 in FIG. 5. When the Read signal on line 110 is activated, the memory 78 accesses the memory location corresponding to the destination address in the AL.sub.-- PA address on bus 108 and supplies the data there to the RX Port State Machine via Data bus 112. This data is a 1 if the destination is local and is a 0 if the destination is remote. This data causes RX Port State Machine to control the Switch Control signal on line 622 so as to set Switch 614 to a 1-3 connection if the destination is local, as represented by path 742 out of step 740 on FIG. 8C, or a 1-2 connection if the destination is remote, as represented by path 744.

Current US Cross Reference Classification (5):
709/214

Current US Cross Reference Classification (6):
709/216

Current US Cross Reference Classification (7):
709/249

☐ 9. Document ID: US 5710941 A

L10: Entry 9 of 11 File: USPT Jan 20, 1998

DOCUMENT-IDENTIFIER: US 5710941 A
**** See image for Certificate of Correction ****
TITLE: System for substituting protected mode hard disk driver for real mode driver by trapping test transfers to verify matching geometric translation

Detailed Description Text (28):
At step 86, protected mode hard disk driver 50 further examines the recorded input/output port accesses to verify whether real mode hard disk driver 48 utilizes a data transfer mode with no geometry translation. To verify that no geometry translation occurs, protected mode hard disk driver 50 compares the data written by real mode hard disk driver 48 to ports 1F3-1F6h against the cylinder, head and sector address of its INT 13h read request. As described above, the cylinder, head, and sector addresses of the INT 13h read request and those of the port access will match for all addresses only if no geometry translation occurs. Accordingly, protected mode hard disk driver 50 determines that real mode hard disk driver 48 does not utilize geometry translation only if both of these cylinder, head, and sector addresses match in all iterations of the loop 80-87. If the cylinder, head, and sector addresses are found to match for all iterations of the loop 80-87, protected mode hard disk driver 50 also utilizes data transfers with no geometry translation when substituted for real mode hard disk driver 48 as indicated at step 88, and verification method 70 ends at step 89. Otherwise, if the addresses are found not to match in any iteration of loop 80-87 which indicates that some form of geometry translation is utilized by real mode hard disk driver 48, protected mode hard disk driver 50 proceeds to steps 90-98 (FIG. 4A).

Current US Cross Reference Classification (1):
709/321

☐ 10. Document ID: US 5371867 A

L10: Entry 10 of 11 File: USPT Dec 6, 1994

DOCUMENT-IDENTIFIER: US 5371867 A
TITLE: Method of using small addresses to access any guest zone in a large memory

Detailed Description Text (36):
The ZN value in R1 is used to index into ZIT 44 to access a ZIT entry associated with the zone of the guest being accessed. Adder 49 is a 64 bit adder which adds a zone origin obtained from the ZIT entry to the small guest address in the R3 register 43, resulting in a 63 bit absolute address which is provided to a comparator 45 which compares the generated absolute address to a zone limit obtained from the ZIT entry. If the absolute address is less than the ZIT entry's zone limit (the normal case), the absolute address is stored in the CPU window specification table entry 47 located with the WR number supplied by R1 42. If the absolute address is larger than the zone limit, an exception small address value is outputted by a register 46 into the CPU window specification table entry 47, and an exception signal is generated to interrupt the CPU. The absolute address value loaded into the CPU window specification table entry 47 is then loaded into the window register 48, which now contains the large address which will be substituted for the guest small address whenever the associated window PF is addressed by a host instruction.

Current US Original Classification (1):
709/100

Term	Documents
COMPAR$	0
COMPAR	3614
COMPARA	4023
COMPARAATIVE	3
COMPARAATOR	5
COMPARABALE	5
COMPARABE	7
COMPARABEL	1
COMPARABIE	1
COMPARABIITY	1
COMPARABILITIES	6
(L1 AND ((COMPAR$ WITH ADDRESS$) SAME (SUBSTITUTE$ WITH ADDRESS$))).USPT.	11

There are more results than shown above. Click here to view the entire set.

Display Format: KWIC Change Format

Previous Page Next Page